POLICY ON USE OF COMPUTING RESOURCES

Document Name	Policy on Use of Computing Resources
Language(s)	English
Responsible Unit	UGC Standing Committee on Computing
Creator (individual)	UGC Standing Committee on Computing
Subject (taxonomy)	Computer Resource Management, Acceptable Use
Date created	22 March 2012
Date adopted	31 December 2012
Mandatory Review	January 2014
Audience	These policies and procedures are to be used by all higher educational institutions, its authorities, staff, students and other operational units.
Replaces	None
Is part of	Computing Policies and Standards
Related documents	Use of IT Policy of the UGC of the HEIT Unit/IT Policy, Version 1.1, August 2007

Version	Date	Author(s)	Revision Notes
1	22 March 2012	UCSC – Mr. C.M.B. Attanayake & Prof. G.N. Wikramanayake	First version V0.10
2			

TABLE OF CONTENTS

SECTION 1. INTRODUCTION

Higher education institutions promote the use of computing to share information and knowledge in support of academic, administrative and management activities. This document establishes the framework for the overall Policy and the standards for higher education institutions regarding the use of computing resources and data.

SECTION 2. GENERAL PROVISIONS

2.1 Reason for Issue

Computing resources are intended to support higher education institution activities and to enable closer and timelier communications, within institutions, University Grant Commission (UGC) and between institutions, staff, students, academia and all other stakeholders. Inappropriate use of these resources can, however, harm an institution, other establishments and individuals. This Policy is intended to minimize the likelihood of such harm by educating institution computing users and by setting principles that will limit financial, operational or legal risk to all parties while safeguarding the institution. The main purposes of this Policy are to:

a. Ensure that institution resources and data are used for purposes appropriate to the institution mandate;

b. Inform users about the applicability of policies to computing resources and data, and ensure they are used in compliance with institution policies;

c. Establish policy on confidentiality, integrity, availability and privacy in computing resources and data;

d. Prevent disruptions to and misuse of institution computing resources, services and activities.

2.2 Scope

This policy shall apply to:

a. All institution staff members, students and associates;

b. All computing resources owned or managed by institution or provided by institution through contracts and other agreements with the institution;

c. All institution computing records in the possession of institution staff, student or of other users of computing resources provided by the institution;

d. Emerging technologies that supplement or extend the capabilities of the computing resources;

e. All computing contents and to the electronic attachments and transactional information associated with such communications.

2.3 Definitions

Annex A contains key definitions that apply to this Policy. An understanding of these definitions is essential to fully comprehending this Policy.

2.4 Responsible Office

This Policy is issued by the UGC computing standing committee. Each institution is responsible for implementation of this Policy. The head of the institution or its authorities (e.g. faculty) is responsible for the implementation of this Policy utilizing standards and guidelines associated with this document.

SECTION 3. CONDITIONS APPLICABLE TO USE OF COMPUTING RESOURCES AND DATA

While an institution actively promotes the use of computing resources and makes them widely available to the user community, institution must limit the use of computing resources by imposing restrictions that apply to all institution property and by establishing constraints necessary for the reliable operation of computer systems and services.

3.1 Allowable Users

3.1.1 Institution Users

Institution employees, students, visiting associates with written authorization/agreement by the head of the institution or sub-unit to work as staff or to, use institution computing resources and services for purposes in accordance with this Policy. Institution users are granted access to computing resources and data through established access control procedures. The principles outlined in this section are applicable to any form of electronic communication. Specific standards and guidelines for users of computing resources are as follows:

a. There are two types of user identities; User Accounts and Service Accounts:

- User Accounts are accounts created for official use. These accounts are setup for individual use by institution staff, students or Associates;
- Service Accounts are accounts created specifically to enable a group of authorized user account holders to gain access messages or services addressing institution needs rather that those of a specific individual (e.g. info, admin, registrar, director). The establishment of these accounts requires the prior approval of the head of the relevant unit (VC/Director/Rector/Dean/Head of the department). These accounts will be created by the computing center of the institution.

b. There are three types of email address classifications for the institution staff, students and affiliates:

- All institution staff members (current & emeritus) shall utilized XXX@XXX(.XXX).XXX.ac.lk (e.g. gnw@ucsc.cmb.ac.lk) naming convention;
- All students shall utilize RegNumber@student.XXX.XXX.ac.lk (e.g. 0700003@student.ucsc.cmb.ac.lk) naming convention;
- All members of the alumina shall utilize RegNumber@alumini.XXX.XXX.ac.lk (e.g. 0700003@alumni.ucsc.cmb.ac.lk) naming convention;

c. User accounts are setup specifically for the purpose of performance of institution activities. As such, these accounts shall be, at a minimum, kept as long as the person to whom the account is assigned is continuing to conduct institution activities. Termination of the account will be effected only as stated below and shall apply to the XXX.ac.lk domain.

- For institution staff the following shall apply:
    - When on long term leave, sabbatical, vacation, the account will continue to be active;
    - When on secondment, the account will be active;
    - When being terminated /separation due to early or normal expiration of contract, the account will be kept active for a period of 60 days from the date of separation;
    - When being terminated subject to dismissal or separation for disciplinary actions, the account will be closed on the date of termination;
    - When retiring from the institution, the account will be kept active for a period of 120 days from the date of retirement;
- For students the following shall apply:
    - When being separation due to Graduation or completing studentship 60 days after graduation or completion of the course.
    - When being terminated subject to disciplinary actions the account will be closed on the date of termination;

- Or any other condition does not mention above the accounts will be closed on the date of separation

- For alumina the following shall apply:
    - Deceased or withdrawal of membership the account will be closed on the date notified /effective of withdrawal.
    - When being terminated subject to disciplinary actions or membership related issues the account will be closed on the date of termination;
    - Or any other condition does not mention above the accounts will be closed on the date of separation from alumina

It is the responsibility of the respective subunits to coordinate and ensure that the necessary user account actions are promptly taken. Service accounts should contain reference to an active User Account designated as the primary contact and an expiration date equal or less to the contract expiration date of the staff member designated as the primary contact. Notification of account changes or expiration should be sent to both primary and secondary.

3.1.2 Public Users

Users who are not identified by specific individual account are categorized as public users. The Public users may access computing resources and data which are classified as public.

3.1.3 Resisted Public Users

Public users who have resisted with the institution computer systems providing personal information and who are identified by a unique user information (user name, email ID, NIC etc). Resisted public users are permitted to interact with selected systems only. Their registrations are done only on voluntary basis after acknowledging the applicable policy documents. The users shall be given the option to remove their registration as their desire.

3.1.4 Transient Users

Users whose electronic communication merely transits institution facilities as a result of network routing protocols or any other reason are not considered "Users" for the purposes of this Policy. However, the provisions outlined in this Policy are still applicable as is institution’s right to inspect passing traffic.

3.2 Restrictions

Computing resources may be provided by institution, its authorities or functions that support these missions adhering to the following provisions:

3.2.1 Violation of Policies and Guidelines

Users shall not use computing resources in violation of other institution policies or guidelines or breach any national laws. This includes, but is not limited to collecting, downloading, creation, storing or transmitting content, messages or any messages/content that may be reasonably construed as

a. Sexually explicit Offensive, insulting, or profane language;

b. Threatening, harassments, sexual harassment and abuse of authority or other forms of aggravation;

c. Unwelcome or harassing proposition;

d. Defamatory or derogatory comments about individuals or institutions;

e. Ethnic, cultural, religious, gender or racial slurs;

f. Advocate or overtly promote personal political beliefs or those of a political parties;

g. destructive ,dangerous or malicious

h. Perform unlawful activities.

i. Seek to impersonate another person (spoofing).

j. Transmit libelous, slanderous, and defamatory in nature, or abusive messages

k. Any other content or material that may otherwise violate the civil and criminal laws of Sri Lanka.

3.2.2 Commercial Use

The use of institution computing resources for commercial purposes not under the explicit patronage of the institution is strictly prohibited as is any activity resulting in personal financial gain.

3.2.3 Degradation of computing resources

Users should not use institution computing resources in a matter that interrupts or degrades system performance or use significant system resources such as:

a. Use of streaming audio/video facilities for entertainment purposes except those provided by institution for academic purpose or as institution special events and online news sources;

b. Download of music and video files, such as MP3s, except those that are for official, academic use ;

c. Participating in peer-to-peer (P2P) file exchange networks not related to official duties or academic purpose ;

d. Frequent or extended “web-surfing” unrelated to institution activities;

e. Undermine the security, integrity, accessibility of the IT Resources;

f. Hosting sites, content that are not under institution mandate; or

g. Installation of non-approved software which may result in system failures or disruptions.

3.2.4 Representation of Institution

Any usage of institution computing resources is directly traceable to institution and therefore, whether intended by the user or not, represents institution. In this regard:

a. Users of institution computing resources shall not use an institution assigned electronic identity (e.g., containing institution domain”) to register with or participate in on line-auctions, sales, or commercial services and/or investment transactions which are not under the patronage of institution or to register with or participate in discussion groups, chat rooms, bulletin board, web-based games or competitions that are not related to official or academic purpose.

b. Users of institution computing resources shall not give the impression that they are representing, giving opinions, or otherwise making explicit or implicit statements in publicly-accessible electronic forums on behalf of institution or any unit, sub-unit without either being so entitled by virtue of their official role, or by having obtained the prior approval of the head of the institution or relevant unit.

c. Users of institution computing resources may employ an electronic signature that reflects their official title and function in institution. However, disclaimer of responsibility for the content of any message or posting should not be part of the signature.

3.2.5 False Identity and Anonymity

Users of institution computing resources shall not, either directly or by implication, employ a false identity. However, a supervisor may delegate his/her identity to an employee to transact institution official activities for which the supervisor is responsible. In such cases, an employee's use of the supervisor's electronic identity does not constitute a false identity. However, when identity is delegated the supervisor and employee are both responsible for all actions performed using the supervisor’s identity.

3.2.6 Interference

Institution computing resources shall not be used for purposes that could reasonably be expected to directly or indirectly cause excessive strain on its computing resources, or unsolicited interference with others’ use of computing resources. Users of computing services shall not engage in the following:

a. Initiate or forward electronic mail chain letters or their equivalents in other services;

b. Exploit computer systems for purposes beyond their intended scope to amplify a widespread distribution of unsolicited electronic communication;

c. Send an extremely large message (>4MG) or send multiple electronic communications to one or more recipients intentionally with the purpose of interfering with the recipients' use of computer systems and services;

d. Intentionally engage in other practices such as denial-of-service attacks that impede the availability of computing services; or

e. Gain unauthorized access to computers by means of spoofing.

3.2.7 Personal Use

Limited personal use of institution computing resources is permissible as long as it does not:

a. Directly or indirectly interfere with the institution's operation of computing resources;

b. Interfere with performance of official duties;

c. Burden institution with noticeable incremental costs; or

d. Violate the terms of this Policy or any policy.

Personal usage of email accounts and stored data are subject to the same policy and monitoring procedures as those applied to official use. Therefore, users should not have the expectation of privacy in using institution computing resources. Institution is not responsible for any loss or damage of data incurred to or by an individual as a result of personal use of institution computing resources.

3.2.8 Intellectual Property

Institution respects intellectual property rights and strictly adheres to all product-licensing obligations. The contents of all electronic communication shall conform to institution policies regarding protection of intellectual property. Using, downloading, copying or transferring any applications, documents, or programs for which institution does not have a valid license is prohibited.

3.2.9 Copyrights

Users are restricted from violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by institution.

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which institution or the end user does not have an active license is strictly prohibited.

3.2.10 Plagiarism

Institution respects all ideas, views, and opinions, findings by individuals or groups. All publish content must be free from Plagiarism. All staff and students shall conform to institution policies, guidelines regarding Plagiarism

3.2.11 Electronic Approvals/Authorizations

Electronic approvals authorizations such as financial approvals and/or authorizations or the provisioning of computer system or service access issued using institution computing resources which generate a financial or legal commitment for institution are subject to institution policies and procedures governing such transactions. User accounts used for such transaction must not be transfer or shared with other staff members.

3.3 Access Restriction

Access to and use of institution computing services or computing resources may be wholly or partially restricted or rescinded by the institution without prior notice and without the consent of the user as set forth in the access without notification or consent section below. Restriction of access and use under such conditions is subject to the approval of the head of the institution or respective units.

3.4 Ownership of Assets

Institution computing resources, systems and services are the property of the institution. Institution has the right to seize and search any computing resources and records it owns. This applies whether these records are in paper, digital, or other format. Institution also owns all computer records pertaining to the activities of institution created by staff or any individual or institution, whether or not institution owns the computing resources, systems or services used to create or use it. If

management believes that there is a need to seize computing resources and records then it must request approval from the head of the institution or respective units.

SECTION 4. RIGHTS OF USERS OF COMPUTING RESOURCES

Subject to the requirements for authorization, notification, and other conditions specified in this Policy, institution may deny access to its computing services and may routinely inspect, monitor or retrieve electronic communication without notifying or obtaining the consent of the computer record holder.

4.1 Access without Notification or Consent

Under certain circumstances, a computer record holder may be notified by institution prior to or at the time of any inspection, monitoring, or retrieval of the contents of institution computer records in the holder's possession, except as provided for below. Institution shall permit the inspection, monitoring, retrieval or seizure of computer records or assets without the notification or consent of the holder of such records under the following circumstances:

a. When there is substantiated reason to believe that there are violations of institution policies, regulations and rules or national law;

b. When there are emergency circumstances;

c. When there are compelling circumstances; or

d. Under time dependent, critical operational circumstances.

When under the circumstances described above the contents of computer records or assets must be inspected, monitored or retrieved without the holder's notification or consent, the following shall apply:

4.1.1 Authorization

Except in emergency circumstances and pursuant to in accordance with the Emergency Circumstances section below such actions must be authorized in advance and in writing by the vice-chancellor, head of the units. This authority may not be further delegated. Authorization shall be limited to the least perusal principle of accessing only those computer records that are relevant to the allegation or the compelling circumstance.

4.1.2 Emergency Circumstances

In emergency circumstances, the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures described in Section 4.2.1, Authorization, above. The reasons for the emergency circumstances actions should be fully reported on and justified.

4.1.3 Notification

In either case, the responsible authority or designee shall at the earliest possible opportunity that is lawful and is consistent with other institution policies notify the affected individual of the action(s) taken and the reasons for the action(s) taken. Each subunit will publish its practices with regards to monitoring and oversight of computer records and should maintain evidence of how this oversight is conducted.

4.2 Privacy

4.2.1 Expectation of Privacy

The use of institution computing resources is not protected by any guarantees of privacy or confidentiality.

a. Staff members ,students and associates shall have no expectation of privacy in using computing resources, including computers, telephones, cell telephones, laptops, personal digital assistants, or access to the Internet.

b. Where possible, login banners should clearly indicate that there is no expectation of privacy when a user logs onto an institution computer resource.

c. Systems owned and/or controlled by institution are accessible at all times by institution for maintenance, upgrades, or any other business or legal purposes.

d. In the course of their duties, system operators and managers may routinely monitor usage or review the contents of stored or transmitted data or messages to ensure compliance with institution policies.

4.2.2 Personal Information

Institution provides privacy protections for some information that personally identifies an individual. Providing information about, or lists of, institution staff members, students, associates, vendors, contractors or affiliates to parties outside institution is expressly prohibited without the prior authorization of the vice-chancellor, head of the respective units.

4.2.3 Electronically Gathered Data

Except when otherwise provided by institution Policy, users of institution computer systems and services shall be informed whenever personally identifiable information other than transactional information will be collected and stored automatically by the system or service. In no case shall electronic communication that contain personally identifiable information about individuals, including data collected by the use of “cookies" or otherwise automatically gathered, be sold, shared, distributed to third parties without the explicit permission of the individual.

4.2.4 Unavoidable Exposure

During the performance of their duties, personnel who operate and support computing resources need to regularly monitor transmissions or observe certain transactional information and in that process might observe certain transactional information. On these and other occasions, systems personnel might observe the contents of electronic communication. Except as provided elsewhere in this Policy, they are not permitted to seek out the contents or transactional information or contents when where not relevant to the abovementioned purposes, or to disclose or otherwise use what they have observed. Such unavoidable exposure of electronic communication including transactional information is limited to the least invasive degree of exposure required to perform such duties. This exception does not exempt systems personnel from the prohibition against disclosure of personal or and confidential information, except insofar as such disclosure equates with good faith attempts to route an otherwise undeliverable electronic communication to its intended recipients. Another area susceptible to unavoidable exposure by individuals who operate and support computing resources is the discovery of system vulnerabilities or unintended system access. Except as authorized, systems personnel shall not exploit system vulnerabilities or gain unauthorized access to the system. Institution expects all personnel to notify systems owners of any vulnerability they have observed.

4.3 Confidentiality

Any computing data, documents, or information that belongs to institution or its stakeholders that has been deemed confidential is not to be circulated or made available through any electronic means without the prior authorization of the head of institution or unit.

SECTION 5. COMPUTER SECURITY

Institution will make reasonable efforts to provide secure and reliable computing services. Operators of institution computing resources are expected to follow appropriate best practices in providing security of computer records, data, application programs, and systems under their control.

5.1 Breach of Security Controls or Disruptions of Network Communication

Unless otherwise authorized by other provisions of this Policy, no person shall breach or attempt to breach any security controls used by institution to protect computing services or facilities, or any records or messages associated with these services or facilities. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes. Other User prohibited activities include:

- Port scanning or security scanning is expressly prohibited unless prior notification to computer security is made.
- Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is a part of the employee’s normal job/duty.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user’s terminal session, via any means, locally or via the Internet/Intranet/Extranet.

5.2 Authentication and Authorization

computing service providers shall keep up to date with authentication technologies supported by institution and implement them in accordance with Information Security Policies, Procedures, Standards and Guidelines and commensurate with the security requirements of the service, application, or system. Computing service providers shall also implement and employ authorization technologies commensurate with the security requirements of the service, application, or system. Circumventing user authentication or security of any host, network or account is prohibited.

5.3 Password Protection and Accountability

Many of the institution computing resources made available to users are protected by a password. Passwords are assigned to individual persons. The individual to whom a password is assigned is expected to preserve the confidentiality of that password, and is accountable for all actions performed and transactions approved through use of that password. Revealing your account password to others or allowing use of your account by others is prohibited.

In the event a supervisor delegates his/her identity to an employee to carryout institution activity for which the supervisor is responsible, as discussed in section 3.2.5 False Identity and Anonymity, the supervisor must not reveal his/her password to allow the employee to perform delegated functions using the supervisor's identity. This would be treated as a violation of this Policy.

5.4 Encryption

Where appropriate, computer records containing confidential data deemed must be *encrypted* during transit across communications networks. Other communications may be *encrypted* during transit if they are handled upon receipt in conformance with the storage requirements for electronic information resources. Relevant encryptions standards that Users of computing resources are expected to adhere are contained in the institution computing standards and guidelines document.

5.5 Recovery

Providers of computing services shall implement recovery practices adequate to ensure rapid recovery from security intrusions and service interruptions.

5.6 Audit and Monitoring

Providers of computing services shall implement and employ cost-effective audit technologies and practices to help identify security violators and speed up recovery from security violations. The use of such audit technologies and practices shall not conflict with other provisions of this Policy, particularly sections addressing Privacy and Confidentiality.

5.6.1 Audit Trails

All activities conducted through institution -provided computing resources may be recorded in system log files and may be subject to review.

SECTION 6. COMPUTER RECORD RETENTION AND DISPOSITION

6.1 Retention

Computer records are subject to standard Records Management guidelines, which provide guidance to institution units and subunits in administering the retention or disposition of computer records, regardless of the medium on which they are stored.

The system operators /administrators must take necessary steps to protect and properly dispose recordkeeping hardware and media according to the policy on Privacy and Confidentiality. Section and record retention disposition.

6.2 Disposition

Each unit /subunit is responsible for determining the preservation of those computer records that have been identified as having lasting business, financial, academic purpose or historical value to their unit.

SECTION 7. FINAL PROVISIONS

7.1 Fraud

Any individual or institution, whether an authorized User or not of institution computing resources shall not use said resources to commit fraud, either directly or by implication. Any fraud that is detected or suspected must be reported immediately to vice-chancellor or the head of unit, who shall coordinate all investigations. All employees will be held accountable to comply with the institution financial regulations, national law and regulations and to act within the Staff Regulations and Rules.

7.2 Violations of Policy

7.2.1 Applicability

Use of computing resources provided by institution constitutes an agreement to the policies and standards contained in this document, and acceptance of accountability for compliance with them. Violations of these policies and principles, or activities inconsistent with relevant institution Regulations and Rules may be subject to disciplinary actions.

7.2.2 Enforcement

To ensure compliance with the provisions outlined in this Policy institution will establish processes and tools that will automate Policy enforcement and that will allow the monitoring and auditing the use of computing resources.

7.2.3 Investigations

Reviews of violations to this Policy will be investigated according to guidelines and procedures the institution. Violations of the computing Policy may be investigated by institution, to determine if misconduct or other violations of the code of conduct have occurred. Staff members who have been found to violate Policy may be subject to accountability and disciplinary measures.

7.2.4 Liability

Use of institution computing resources which is in contravention of the present Policy and causes financial or other loss to institution, its clients, or its partners may result in the responsible staff member being held personally liable for such consequences. All users prohibit the theft or abuse of computers and other electronic resources such as computing resources, systems, and services. Abuses include (but are not limited to) unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operation of computing resources, systems, and services.

7.2.5 Disciplinary Actions

Institution Policy prohibits the use of institution property for illegal purposes and for purposes not in support of institution mandate. In addition to any possible legal sanctions, violators of this Policy or misconduct may be subject to disciplinary action and/or resulting in suspension of access.

7.2.6 Violations by Non-Authorized Users

Individuals or institutions not authorized to use institution computing resources that have been found to violate this Policy including the commitment of fraud using institution computing resources will be prosecuted to the greatest extent of applicable national law.

7.3 Effective Date

This Policy shall enter into force on 31st December 2012**.**

SECTION 8. ANNEX A: DEFINITIONS

Associates Any visitor who is on official agreement with Institution.

Authorized User Any staff member (see definition below), student or resisted public users who are authorized to use computing resources.

Compelling Circumstances - Circumstances in which failure to act might result in significant bodily harm, significant property loss or loss of significant evidence of violations of institution policies.

Cookie A small file that a Web server automatically sends to your PC when you browse certain Web sites. Cookies contain information that identifies each user so when a user revisits a Web site, the computer automatically establishes the user's identity, thus eliminating the need to reenter the information.

Denial-of-service Attack - A type of attack on a network that is designed to bring the network down by flooding it with useless traffic.

Electronic Communication - Any communication that is broadcast, created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several computer systems or services. For purposes of this Policy, an electronic file that has not been transmitted is not an electronic communication.

Electronic Mail (Email) Account – An account that stores electronic messages on a server by means of an email address and a mailbox. Incoming emails are held in the mailbox. A user can access their mailbox via email software. They can also send email from the mailbox. An email account is password-protected and can be accessed by a computer's email client or by a web-based email application.

Emergency Circumstances - Circumstances in which time is of the essence and there is a high probability that delaying action would almost certainly result in compelling circumstances (see definition above).

False Identity The name or electronic identification of another individual.

Computer Record Holder or Electronic Communication Holder - An electronic communication user who, at a given point in time, is in possession or receipt of a particular computer record, whether or not that computer user is the original creator or a recipient of the content of the record. An individual is in possession of an computer record, whether the original record or a copy or modification of the original record, when that individual has effective control over the location of its storage or access to its content. Thus, a computer record that resides on a computer server awaiting download to an addressee is deemed, for purposes of this Policy, to be in the possession of that addressee. Systems administrators and other operators of institution computing services are excluded from this definition of possession with regard to electronic communication not specifically created by or addressed to them. Computer users are not responsible for computer records in their possession when they have no knowledge of the existence or contents of such records.

Computer Records or Computer Data - Electronic transmissions or messages created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communication systems or services. This definition of computer records applies equally to the contents of such records, attachments to such records, and transactional information associated with such records.

Computing resources - Any combination of tangible or intangible assets such as telecommunications equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation capable of generating, transmitting, receiving, processing, or representing data in electronic form that supports computing services, where the asset is owned, licensed, operated, managed, or made available by, or otherwise used by, the institution.

Computing Service Provider - Any institution, unit or staff with responsibility for managing the operation of and controlling individual user access to any part of the institution’s computer systems and services.

Computer Systems or Services - Any messaging, collaboration, publishing, broadcast, or distribution system that depends on computing resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across computer network systems between or among individuals or groups, that is either explicitly denoted as a system for computing or is implicitly used for such purposes.

Institution Is a higher education institution such as an institution.

Official Use Use of computing resources by an authorized user in performing official functions and within the scope of their authorization.

Personal Use Use of computing resources by an authorized user for other than official purposes and within the scope of their authorization.

Spoofing A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

Staff Member An institution employee as defined by a written contact.

Substantiated Reason - Reliable evidence indicating that violation of institution policies relating to access without notification or consent probably has occurred, as distinguished from rumor, gossip, or other unreliable evidence.

Sub-unit Part of an institution such as faculty, Institute, School, Campus.

Time-dependent, Critical Operational Circumstances - Circumstances in which failure to act could seriously hamper the ability of institution to function administratively or to meet its obligations, but excluding circumstances pertaining to personal or professional activities.

Transactional Information - Information, including electronically gathered information, needed either to complete or to identify an electronic communication. Examples include but are not limited to: electronic mail headers, summaries, addresses and addressees; records of telephone calls; and IP address logs.

Institution Computer Systems or Services - Computer systems or services owned, operated or provided by the institution or any of its sub-units.

Use of Computing Services - To create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic communication with the aid of computing services. An Electronic Communications User is an individual who makes use of computing services. The act of receipt of electronic communications as contrasted with actual viewing of the record by the recipient is excluded from the definition of "use" to the extent that the recipient does not have advance knowledge of the contents of the computer record.

Any questions regarding this Policy may be directed to the Standing Committee on Computing of the UGC.